Campus Operations
Best Current Practices

Campus Network Design & Operations Workshop

These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license (http://creativecommons.org/licenses/by-nc/4.0/)

UNIVERSITY OF OREGON

Last updated 20th October 2022

NSRC
Network Startup Resource Center

Core Network Services

- These are critical for the network to operate correctly. IP packets may flow in the network, but if these services don't reply or aren't configured correctly, users and devices won't be able to connect, and network applications won't be accessible.
- They are:
  1. DNS
  2. DHCP
  3. NTP
  4. Authentication services

Service-by-Service

- In the next slides, we'll explain in turn
  - The importance of each service
  - Guidelines on proper design and configuration
  - How to monitor them

DNS: Domain Name Service

- Without DNS, there is effectively no network.
  - All users, and possibly backend services, are affected (authentication, mail, ...)
- There are two kinds of DNS servers
  - **Caching** (also called resolver):
    - Look up (fetch and return) DNS information for clients
    - "*what's the IP address of www.nsrc.org ?*"
  - **Authoritative**
    - Serve DNS data, reply to queries from Caching servers
    - "*I have the answer to your question, the IP address of www.nsrc.org is 128.223.157.25*"
  - We'll focus on **Caching** DNS service.

DNS Design Recommendations (1)

- Campus networks must offer reliable & fast (low latency) DNS service
  - Have on-campus, fast caching resolvers
  - Virtual machines OK, with enough RAM and CPU to deal with load

- Avoid giving users resolvers which are tens or hundreds of milliseconds away
  - Public service resolvers are usually well intended – but they harm the Internet experience for users, and result in large amounts of DNS traffic using external and transit links

DNS Design Recommendations (2)

- Fast and reliable local DNS caches gives better response times
  - Reduces the amount of DNS traffic that must leave the campus
  - Allows blocking access to undesirable domains (policy or other)
    - Use DNSBL (DNS Blacklist) type services
    - No need for HTTP proxies or DPI (Deep Packet Inspection)

- Give DNS caches **public** IPv4 addresses
  - Avoid placing them behind NAT/firewalls at all costs (even if clients are on private space) as this will rapidly consume NAT resources

DNS Design Recommendations (3)

- If your campus runs authoritative DNS too:
  - Don’t ever use your authoritative DNS as a resolver
  - Use separate system/VM for authoritative DNS
  - If you have Active Directory, then assign it a subdomain of a real domain you own, e.g. ad.myuniv.edu
- Totally different functions – keep them apart!
  - Authoritative DNS is queried by the *world* and gives out information about your domains and your IPv4/IPv6 addresses (reverse DNS)
  - Caching DNS is for your *on-site* users, and keeps cache of frequently used names and addresses

DNS Software & configuration

- We recommend using either **Unbound** or **PowerDNS-recursor** as the caching resolver
  - Both of these are caching only
  - https://nlnetlabs.nl/projects/unbound/about
  - https://www.powerdns.com/recursor.html
- Define which address ranges (v4 & v6) are allowed to use your cache
  - **Only** hosts and devices on the campus!
- No other configuration needed!

DNS Redundancy (1)

- Redundancy is critical
  - Have two caches on campus
- Larger campuses may have two layers of DNS servers
  - Core servers and client facing servers
  - IP addresses of servers for DNS given out using DHCP

DNS Redundancy (2)

- DNS uses a simple client-based failover
  - If DNS1 doesn't answer, wait X seconds and try DNS2
  - For *every* query!
- Be aware of problems this can cause
  - There are ways to mitigate this

DNS Monitoring

- Use a service monitoring tool (Nagios, SmokePing) to monitor availability and latency.

- For each cache
  - Check regularly that a given name can be looked up
    - And the answer is the expected one
  - Verify that the cache answers in a timely fashion
    - For example, below 10ms response time for cached data

Dynamic Host Configuration Protocol (DHCP)

- If DHCP is down, or leases full, new clients can’t access the network!
  - DHCP hands out:
    - IP address and subnet information
    - Default gateway
    - DNS servers to use
    - Configuration server information (e.g. VoIP PBX, TFTP)

DHCP: Design recommendations (1)

- Place DHCP servers near the core
- Configure DHCP relaying on each subnet facing interfaces
- Broadcast DHCP messages from clients are *relayed* to DHCP servers in the core
- To avoid rogue DHCP servers, consider setting up DHCP snooping
  - Blocks DHCP replies from non authorized DHCP servers

DHCP: Design recommendations (2)

- Use DHCP even for fixed IP addresses (static leases)
  - Renumbering is easier
- Lease times of a few hours are ok
  - Reclaim IP addresses faster if clients leave network without releasing
- For IPv6: turn off SLAAC and use DHCPv6 if possible
  - SLAAC is “stateless autoconfiguration” – the router on the subnet tells the client what the subnet and default gateway are
    - No longer a relationship between the client and the IP address recorded on a central system as for DHCP, which makes troubleshooting much harder
  - DHCPv6 operates similarly to DHCP for IPv4

DHCP: Software & configuration

- We recommend something well known like ISC-DHCPD
- Configuration is not very difficult, but there are many options.

DHCP: Redundancy

- For reliable DHCP, you need a pair of servers.
- Setting up redundant DHCP service isn't covered here
  - Either have each server cover ½ subnet range
  - or have full failover and synchronization, which is complicated

DHCP: Monitoring

- Keep an eye on the log files
  - Using, say, **tenshi**
- Look for warnings about pool usage
  - Are the ranges allocated about to be full?
- Network equipment can warn of rogue DHCP servers
  - See DHCP snooping

NTP – Network Time Protocol

- Accurate time keeping is critical for the network to function properly, and to maintain synchronized logs across devices
  - If clocks are off, some authentication protocols, and DNS, may fail
  - Matching log information with incorrect timestamps is very time consuming
  - Use consistent timezones: either UTC or your local time zone
- In case of a security incident, you may need to:
  - Match DHCP log with NAT entries locally
  - And match those with information sent by a remote site administrator

NTP: Design Recommendations

- For precise timekeeping, it's not recommended to run an NTP server inside a virtual machine
- NTP servers can live on the same servers as the DNS resolvers and DHCP servers.
- Be aware that unpatched software can turn misconfigured NTP servers into attack amplifiers
- If you are running a pair of ID management/DS servers (Active Directory) then they can, and probably already do, act as your DNS, NTP and DHCP servers.

NTP: Software & configuration

- NTPD is well known but has a history of security issues.
- It may be worth looking at Chrony or OpenNTPD.
- If there is a stratum 1 NTP clock nearby (local exchange point for example) then you can use that.
  - But it's also good enough to use pool.ntp.org
- Not all OSes and devices allow having more than one NTP server listed!

Authentication servers

- Many possibilities, you might have:
  - User database: Active Directory, FreeIPA, LDAP, SQL...
  - RADIUS server (802.1x wireless authentication)
  - Captive portal
  - ...
- Users cannot access the network without them
- Have replicated instances, preferably live-live
- Implement active monitoring (e.g. Nagios plugins)

Other recommendations (1)

- We could fill a book with these, so here a few essential things worth considering
- Implement anti-spoofing (BCP38) at the border of your campus
  - Don’t allow packets with source IP addresses other than from your own address space to exit your campus
  - Check that your NAT (if used) only translates address space used internally in your campus
    - A common mistake is to translate any and every source IP address
  - https://www.manrs.org/

Other recommendations (2)

Block connections to port 25/TCP outbound except from the official trusted email servers

- Configure other servers, and clients, to use those for outbound email
- This gives you better control and insight into how mail is being (ab)used
- With anti-spam and anti-virus controls on the mail server, this helps prevent the campus address space landing in spam blacklists

- **Note**: Users who are using public mail services will send their email via submission protocol (587/TCP) or 465/TCP
  - Requires authentication first before sending is possible
  - No end user ever needs to send email using 25/TCP

Other recommendations (3)

Consider rate limiting UDP (except for known video conferencing devices) to slow down bit-torrent

- Blocking bit-torrent over UDP entirely will simply make it switch to TCP
- Bit-torrent will also tunnel using IPv6 if the option is selected in the client

Other recommendations (4)

- How to access network devices and servers when the IP connectivity has failed due to:
  - IP network down
  - Infrastructure power outages
  - Human error
- By using Out of Band (OOB) management devices
  - Serial/USB ports connect to serial/USB ports of network devices (and servers)
  - Ethernet to core network
  - Some offer options for 4G LTE, dialup modem, etc

Out of band (OOB) Management

- Using OOB device is quicker than going to the location with a laptop and serial cable to access the device console
- The most commonly used OOB devices include:
  - OpenGear's CM7100 (16-96 serial ports)
  - OpenGear's ACM7008-2
    - https://opengear.com/products/acm7000-resilience-gateway
  - AirConsole TS
    - https://www.get-console.com/shop/en/24-device-servers

Out of band Management

- Alternatively, build an out of band solution yourself
  - Simple Linux PC (mini-PC is sufficient)
  - Multi-port USB hub
  - USB to serial cables

- Out of band access to network devices is essential to rapidly resolve issues
  - Highly recommended!

Questions?

This document is a result of work by the Network Startup Resource Center (NSRC at https://www.nsrc.org). This document may be freely copied, modified, and otherwise re-used on the condition that any re-use acknowledge the NSRC as the original source.